A. JOSEPH DeNUCCI
AUDITOR

The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH
ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108
TEL. (617) 727-6200

No. 2001-1413-4C

INDEPENDENT STATE AUDITOR'S
REPORT ON THE EXAMINATION OF
INFORMATION TECHNOLOGY-RELATED CONTROLS AT THE
HUMAN RESOURCES DIVISION

JULY 1, 2000 through OCTOBER 19, 2001

OFFICIAL AUDIT REPORT
DECEMBER 19, 2001

2001-1413-4C

TABLE OF CONTENTS

INTRODUCTION

The Human Resource Division (HRD) is authorized under Chapter 7, Section 4A of the Massachusetts General Laws as amended by Chapter 151, Section 25 of the Acts of 1996. The Division resulted from the consolidation of the former Department of Personnel Administration, the Office of Employee Relations, Office of Workers' Compensation, and the Office of Affirmative Action. The Division serves as the central personnel department and provides human resources services to the executive branch of state government. In addition, HRD administers the Commonwealth's civil service system for both state agencies and many local government communities covering operational areas, such as public safety.

The primary mission of the Division is to develop a comprehensive plan for the delivery of human resources throughout state government and municipal sub-divisions and establish the structure within which human resource management can be effectively performed. The Division provides the technical assistance, training, and oversight needed to ensure that the Commonwealth's classification, compensation, recruitment, selection, training and employee development, civil rights, collective bargaining, and workers' compensation programs are carried out in a coordinated and streamlined manner that results in a timely and efficient service within the Executive Office of Administration and Finance. Approximately one hundred and sixty-seven employees, temporary staff, and consultants serve the multiple operating units with one executive office at Ashburton Place.

The Division's business processes are supported by information technology (IT) resources managed by HRD and the Commonwealth's Information Technology Division. IT operations internal to HRD are supported by a local area network (LAN), microcomputer workstations, and 40 laptop computers that are either permanently assigned or available for assignment. The Division's mission-critical application (the workers' compensation system) is operated on a Wang VS minicomputer. The HRD will replace the application system and the hardware platform in the near future. The Division's essential system, Electronic and List Information Processing System (ELIPSYS), is operated on a mainframe computer system that is managed by the Commonwealth's Information Technology Division in Chelsea.

The Division's LAN consists of five file and application servers operating in a Microsoft NT environment. Application servers include the HRD domain controller, Microsoft Exchange mail server, Microsoft SQL server, and Internet Information Server, and a print server. The HRD is supported by approximately 200 microcomputers. A training server and 68 training microcomputers are in use within the executive office at One Ashburton Place. HRD accesses from their desktop microcomputer workstations the ELIPSYS and MMARS mainframe application systems residing on the Massachusetts Information Technology Center's data center. The HRD uses a variety of business-related software to communicate with and support its customers and other HRD departments within the Commonwealth.

The Division uses Microsoft Office Professional and other Microsoft productivity products as its standard desktop software platform.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

From March 28, 2001 through October 19, 2001, we conducted an IT audit at the Human Resources Division (HRD) for the period of July 1, 2000 through October 19, 2001. The scope of the audit included an examination of IT-related controls pertaining to organization and management, physical security, environmental protection, fixed-asset inventory for the IT environment, logical access security, disaster recovery and business continuity planning, and on-site and off-site storage of backup magnetic media for mission-critical and essential computer systems.

Audit Objectives

We sought to determine whether organization and management's planning included sufficient oversight over the operations of the division. In addition, we sought to determine whether there were sufficient security controls and environmental protection over the physical plant. We sought to determine whether access to applications at the ITD mainframe computer and the Division's in-house minicomputer systems were adequately restricted to authorized users in order to prevent unauthorized access, use, damage or loss of computer equipment or IT-related media. We also sought to determine whether sufficient inventory controls were in effect to properly account for computer equipment. In addition, we sought to determine whether adequate disaster recovery and business continuity plans were in place to provide reasonable assurance that IT functions could be regained within an acceptable period of time should a disaster render the Division's IT systems inoperable or inaccessible. We also sought to determine whether adequate media backup procedures were being performed and whether copies of mission-critical and essential IT-related magnetic media were stored in secure on-site and off-site locations.

Audit Methodology

To determine the areas to be examined during the audit, we reviewed relevant enabling legislation; obtained and recorded an understanding of the Division's mission, organization, and business objectives; conducted interviews with senior management; and conducted a pre-audit survey and preliminary review of internal controls pertaining to IT-related organization and management, physical security, environmental protection, logical access security, disaster recovery and business continuity planning, and on-site and off-site storage of backup magnetic media.

We sought to determine whether users of the computer systems were accurately identified and were employees who had been authorized to have appropriate levels of procedures as authorized and required

to accomplish their assigned duties. We also determined whether all laptop computers had been properly identified, correctly recorded on a perpetual inventory record, and could be located within the entity's main or alternate site(s).

We sought to determine what disaster recovery and continuity plans existed and assessed their adequacy to ensure continuity of operations if either a complete system failure or the failure of system components occurred. We determined whether procedures were in place to provide for the recovery of files, address disaster recovery, and identify critical processing data. We reviewed the plan to determine whether it allowed for periodic testing (at least annually or upon major changes to the IT infrastructure), to ensure personnel understand their respective roles during a disaster and validate the plan and the provisions for the backup of critical information and materials both on-site and off-site.

To assess the reliability of disaster recovery and business continuity planning, we determined whether recovery and continuity plans existed and whether the recovery strategies incorporated appropriate information to help ensure that mission critical and essential operations and business functions could be re-established. We also determined whether the disaster and recovery plan addressed various scenarios that would render it inoperable.

AUDIT SUMMARY

Based on our audit at the Human Resources Division (HRD), we found that there was reasonable assurance that IT-related control objectives would be met by internal controls in place with respect to IT organization and management, physical security, environmental protection, and on-site and off-site storage of backup magnetic media. However, we found that certain IT-related controls needed to be implemented or strengthened regarding logical access security, fixed-asset inventory, and disaster recovery and business continuity planning.

Our review of internal controls indicated that the Division had a defined organizational structure, clearly delineated reporting responsibilities, documented job descriptions, and management awareness of internal control. We found that the HRD had developed an "Internal Control Plan" to comply with Chapter 647 of the Acts of 1989.

Our examination of physical security and environmental protection determined that controls provided reasonable assurance that control objectives related to general housekeeping; for temperature and humidity levels, smoke detection, fire prevention, detection, and suppression; and emergency lighting were in place to safeguard IT-related resources in the mainframe, minicomputer, and file server areas in Boston and Chelsea. In addition, we found that appropriate controls were in place for off-site storage of computer media.

We found that system access security over the HRD's mainframe and minicomputer systems needed to be strengthened to ensure that access to systems, data, and programs is restricted to only authorized users and to safeguard information against unauthorized use, disclosure, or modification. Procedures need to be enhanced to ensure timely action related to suspending and/or closing user accounts.

Although there were informal procedures in place, there were no written policies and procedures to inform the security administrator when an employee, consultant/contractor, or other user terminated employment, and notification was not always provided to the system security administrator. Further, the procedures for establishing an audit trail of activating and deactivating user accounts needs to be strengthened to provide adequate documentation. Our tests of access security for the mainframe and minicomputer indicated that, contrary to sound access security practices, there were active user IDs for individuals who were no longer employed by the Department. Our tests of the mainframe and minicomputer indicated that two (or 1.4%) out of 141 users were not current employees or contractor personnel.

Our review of the policies and procedures regarding fixed-asset inventory indicated that the policies for conducting inventory could be strengthened. We found that an inventory system of fixed assets had

been maintained, but the physical inventory had not been reconciled to the inventory system, which could result in inventory records being inaccurate and incomplete.

Our initial tests of all fifty laptops revealed that management was unable to locate five laptops costing $13, 647. Our subsequent tests of HRD's inventory record, consisting of a judgmental sample of 32 hardware items out of the fixed-asset inventory which totaled 700 items, revealed that all of the tested assets were in the location indicated on the inventory listing. Although in our initial tests the Division did not know that five laptops were missing, we acknowledge that HRD has since reported the lost laptops to the OSA, as required by Chapter 647 and has updated their inventory to include the laptops on the inventory as missing.

We found that HRD had developed a comprehensive business continuity plan that outlined a sound strategy for maintaining system availability in the event of a major disaster or disruption of IT operations. Furthermore, the Division's documented procedures, if followed, provided reasonable assurance that IT operations could be recovered should IT equipment become damaged, inoperable, or inaccessible. Although we noted that the plan had been tested, we found that the business continuity testing criteria include loss of services for only one day. We recommend that the HRD continue to test its disaster recovery and business continuity plan on a regular basis and include scenarios for loss of services for a week, two weeks, a month, or more. We also recommend that a process be established for routinely updating the plan based on changes to the technology, business processes, staffing, or threats and vulnerabilities to the IT processing environment. We found that appropriate procedures were in effect for making backup copies of magnetic media and for storing the backups on-site as well as at off-site locations in Boston and Chelsea. In addition, we found that the storage facility housing on-site backup copies of computer-related media was adequately safeguarded and environmentally protected.

AUDIT RESULTS

1. Logical Access Security

Our audit revealed that system access security over the HRD's access to ITD's mainframe and HRD's minicomputer systems needed to be strengthened to provide reasonable assurance that access to systems, programs, and data files is restricted to only authorized users and to safeguard information against unauthorized use, disclosure, or modification.

At the beginning of the audit, although we found that policies and procedures were generally documented for HRD, IT related functions, policies and procedures regarding access security needed to be more fully documented. For example, we noted that although there were informal procedures in place, there were no written policies and procedures to inform the security administrator when an employee or consultant/contractor or other user had terminated employment, and notification was not always provided to the system security administrator. As a result, we found that system access security procedures needed to be enhanced to ensure timely action related to suspending and/or deactivating user accounts. Although we found that adequate procedures were being followed to authorize users and activate user access privileges, the procedures for establishing an audit trail of activating and deactivating user accounts needed to be strengthened to provide adequate documentation. Our tests of access security for the mainframe and minicomputer indicated that there were two active user logon IDs for individuals who were no longer employed by the Division. Our tests of the mainframe and minicomputer indicated that two (or 1.4%) out of 141 users were not employees or contractor personnel. These former staff left the Division over twelve months ago, yet their IDs still remained active. We note that when this information was brought to management's attention, corrective action was taken immediately. Sound access security practices would have detected the presence of active user accounts for individuals no longer authorized or requiring access to authorized systems.

Recommendation:

In order to improve system security at HRD, the following steps, at a minimum, should be performed:

- Establish a mechanism for documented notification to the security administrator when user access privileges should be changed or deactivated.
- Review documented policies and procedures regarding access security to determine whether they are appropriate and sufficiently documented and make any necessary modifications.
- Ensure that there is an adequate audit trail for activating and deactivating user accounts.

- Remove, as soon as possible, user IDs of those individuals identified as no longer current staff or contractors.
- Notify security administration by e-mail of terminations or leaves of absences of all appropriate staff in order to further decrease the chance of an account remaining active following the separation of an employee from HRD. A copy of the e-mail notifying termination should be maintained in the Employee Relations files and the supervisor's files. By maintaining these records, the Division will have established an audit trail to assist in performing reviews of active system users.
- Based upon HRD's assessment of risk and established level of assurance that access security control objectives are being addressed, Division management should determine the frequency of required reviews of user IDs to the list of authorized users. We suggest that the review of user IDs be performed at least semi-annually.

Auditee's Response:

HRD understands the importance of Logical Access Security and welcomes the logical access security recommendations contained in this report. Prior to the audit, HRD had documented logical access security procedures in the HRD Internal Control Plan and separately in other documents. However, HRD agrees with the recommendation that these procedures can be tightened, particularly in the area of written procedures for notifying the system security administrator when employees terminate their employment with HRD. Though the audit found that only 2 of 141 (1.4%) names on our access control lists should have been deactivated, this represents a breach of security that is unacceptable to HRD management. Therefore HRD has already taken or will take the following steps to improve system access security:

During the audit, HRD revised and adopted procedures for notifying the appropriate staff when an employee is terminated. These revised termination procedures document a formal mechanism for notifying the HRD CFO when an employee terminates employment with HRD. The CFO then uses a standard form for notifying MMARS Security Administrator, the HRD Network Manager and the HRD Physical Security Officer of the imminent termination. Only after these individuals verify that all logical and physical security access has been revoked and all HRD property returned, does the HRD CFO authorize the release of the employee's last paycheck. A copy of these revised procedures is attached to this response.

HRD has reviewed and will continue to review our documented procedures regarding access security to determine if they are appropriate and sufficiently documented or require additional modification. This will be incorporated in the annual review of the HRD Internal Control Plan.

HRD will ensure that there is an adequate audit trail for activating and deactivating user accounts. E-mail and the termination checklist form will be used to create an audit trail.

The revised termination procedures developed by HRD address the need to remove as soon as possible user ID's of individuals no longer employed at the agency.

HRD will revise the termination policy to require notification of leaves of absence or termination by e-mail and will require a copy of the e-mail to be maintained in the Security Administrator's file, the Employee Relations File and the supervisor's file.

HRD will conduct an audit of system access user lists based on the list of active HRD employees on a semi-annual basis.

Taken together, HRD believes that these measures in concert with the system access security procedures already in place will adequately addresses the agency's system access security needs.

Auditor's Reply:

We are pleased that the HRD has already taken or will take steps to improve system access security. We acknowledge that the HRD has taken sound steps to improve procedures for establishing an audit trail of activating and deactivating user accounts (including the removal of user ID's of individuals no longer employed), for new notification procedures for leaves and or termination, for procedures to semi-annually audit the user list, and for procedures to annually review the HRD internal control plan. We will review how these procedures are followed during our next audit.

2. Inventory Control

Our review of the policies and procedures regarding fixed-asset inventory indicated that the policies for conducting inventory needed to be strengthened. We found that an inventory system of fixed assets had been maintained, but the physical inventory had not been reconciled to the inventory system of fixed assets, which could result in inventory records being inaccurate and incomplete.

Our initial tests of the inventory record focused on IT resources that would be considered as portable. Our review of all fifty laptops listed on the inventory record revealed that HRD was unable to locate five laptops valued at $13,647. In our initial tests, the Division did not know that the five laptops were missing. We acknowledge that HRD has since reported the lost laptops to the OSA, as required by Chapter 647 and has updated their inventory to include the laptops on the inventory as missing.

The laptops were not recognized as missing partly because HRD confirmed its annual physical inventory to a desktop equipment database, which was easily verifiable and did not include a confirmation of laptop computers, which were often at employees' homes. Another contributing factor was the failure to keep a sign-out sheet up to-date for the removal of laptops from HRD headquarters.

Our subsequent expanded tests of HRD's inventory record, consisting of a judgmental sample of 32 hardware items selected from the fixed-asset inventory system of record, which totaled 700 items,

revealed that all of the tested assets were in the physical location indicated on the inventory listing. Additional tests determined that IT resources purchased from fiscal year 1999 through the audit period were properly recorded. In addition, we found that 15 items of IT equipment judgmentally sampled from their physical locations were also properly recorded on the inventory record.

Recommendation:

To ensure that the inventory of IT resources is adequately maintained, we recommend that HRD enhance its policies and procedures to include reconciling the physical inventory to the fixed-asset inventory at least annually. We also recommend that the policies and procedures for the reconciliation of laptop computers be more frequent than annually and that they include more controls over the movement of laptops including signed documentation regarding the responsibilities for use and reporting. We further recommend that the Division ensure that the physical inventory is reconciled to the fixed-asset inventory so that the record can be appropriately updated and verified for accuracy. Also the sign-out sheet for the removal of laptop computers should be up-to-date.

Auditee's Response:

HRD understands the importance of Inventory Control procedures and welcomes the Auditors' recommendations contained in this report. Prior to the audit, HRD had documented policies and procedures for inventory control that included the annual physical inventory of all IT equipment, maintenance of sign-in and sign-out documents for laptop computers, procedures for purchasing IT equipment and for incorporating purchased equipment into the inventory. The audit revealed that all desktop equipment tested was properly purchased, tagged and located. Unfortunately, the audit also revealed that 5 older laptop computers could not be accounted for. As a result of this finding, HRD will take or has already taken the following steps:

HRD will review and enhance all of its policies and procedures that relate to the reconciliation of its physical inventory to our fixed assets inventory.

HRD has already significantly enhanced our policies and procedures regarding the inventory and control over the movement of laptop computers. During the audit, HRD developed and adopted a revised set of Procedures for the Storage and Handling of Laptop Computers. (attached). These revised procedures provide for:

Enhanced physical security over all laptop computers. All laptops will be organized in one physical location in a locked cabinet in the locked server room.

Enhanced Laptop Sign out procedures. Responsibility for the sign-out and receipt of laptops is now solely the responsibility of the Network Administrator. (In the past more than one person was responsible for this activity). The network Administrator is also solely responsible for the maintenance and currency of sign-in and sign-out sheets.

Written procedures for signing out and signing in laptops have also been enhanced. These procedures will assist HRD's Network Administrator to ensure that the sign-out sheets are complete and up to date.

Inventory tracking procedures for laptops have been significantly enhanced. On a semi-annual basis, the Network Manager will run a report from the inventory database of all laptops currently in house and on-loan. These reports will be verified by checking the logbook and the physical inventory of laptops on site. Any discrepancies will be identified to the CIO and resolved.

Physical inventory procedures for laptops have been significantly enhanced. Once every 6 months all employees using a loaned laptop will be required to respond to e-mail from the Network Manager identifying laptop manufacturer, serial number and HRD tag number. Physical recall of laptops will be required on an annual basis for visual inspection.

Taken together, HRD believes that these measures in concert with the inventory control procedures already in place will adequately addresses the agency's inventory control needs.

Auditor's Reply:

We are pleased that the HRD understands the importance of inventory control procedures and that HRD will take or has taken the steps to review and enhance policies and procedures that relate to the reconciliation of your physical inventory to the fixed assets inventory, that HRD has enhanced policies and procedures regarding the inventory and control over the movement of laptop computers, including: a recently developed and adopted a revised set of procedures for the storage and handling of laptop computers; and has enhanced laptop sign out procedures. We agree that these procedures will assist HRD's Network Administrator to ensure that the sign-out sheets will be accurate, complete and up to date.

We commend the HRD for taking measures to address the agency's inventory control needs. We will review how these procedures are followed during our next audit.